AO-106 (Rev. 06/09)-Application for Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

FILED
SEP 05 2023
Mark C. McCartt, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of
one black dell laptop with product key TBFWD-W749M-QIXVR-MWKEW-CW6T3, and six thumb drives described as follows: one plain metal swivel thumb drive, one Kingston brand thumb drive with orange and black lanyard, one PNY brand black plastic optima pro 4gb thumb drive, one Kingston brand thumb drive with metal finish, one Kingston brand thumb drive with a Shawnee Public Schools label, and one purple Lexar brand thumb drive 8gb, all of which are currently located at FBI Tulsa Resident Agency property room, 8023 East 63rd Place, Tulsa, Oklahoma

Case No. 23-MJ-476-SH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):* See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):* See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1151, 1153, and 2241(c)	Aggravated Sexual Abuse of a Minor Under 12 Years of Age in Indian Country
18 U.S.C. §§ 1151, 1153, and 2244(a)(5)	Abusive Sexual Contact of a Minor Under 12 Years of Age in Indian Country
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	Possession of and Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of Steven Colon, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SCC

Applicant's signature

Steven Colon, Special Agent, FBI

Printed name and title

Subscribed and sworn to by phone.

Date: 9/5/23

Judge's signature

City and state: Tulsa, Oklahoma

Susan E. Huntsman, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of one black dell laptop with product key TBFWD-W749M-QIXVR-MWKEW-CW6T3, and six thumb drives described as follows: one plain metal swivel thumb drive, one Kingston brand thumb drive with orange and black lanyard, one PNY brand black plastic optima pro 4gb thumb drive, one Kingston brand thumb drive with metal finish, one Kingston brand thumb drive with a Shawnee Public Schools label, and one purple Lexar brand thumb drive 8gb, all of which are currently located at FBI Tulsa Resident Agency property room, 8023 East 63rd Place, Tulsa, Oklahoma	**Case No. _____**

Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize

I, Steve Colon, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—seven electronic devices as described in Attachment A—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Tulsa Resident Agency (RA) and have been since July 2018. Prior to being a Special Agent with the FBI, I was an Active Duty United States Marine for 20 years. Currently, I am assigned to conduct investigations pursuant to the FBI's Safe Trails Task Force (STTF), which focuses on myriad crimes occurring on Indian reservations to include sexual assaults of minors and production of child pornography. I have received basic and on-the-job training in the investigation of cases involving sexual assaults of minors and production of child pornography.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 1151, 1153, and 2241(c) (Aggravated Sexual Abuse of a Minor Under 12 Years of Age in Indian Country, 18 U.S.C. §§ 1151, 1153, and 2244(a)(5) (Abusive Sexual Contact of a Minor Under 12 Years of Age in Indian Country), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) will be located in the electronically stored information described in Attachment B and is recorded on the Devices described in Attachment A.

Identification of the Devices to be Examined

5. The property to be searched is described below, hereinafter the "Devices." All of the Devices are currently located in the FBI Tulsa Resident Agency Property Room located at 8023 East 63rd Place, Tulsa, Oklahoma, within the Northern District of Oklahoma. An image of Devices b-g are located in Attachment A.

a. Black Dell Laptop computer, product key TBFWD-W749M-QIXVR-MWKEW-CW6T3;

b. One plain metal swivel thumb drive;

c. One Kingston brand thumb drive with orange and black lanyard;

d. One PNY brand black plastic optima pro 4gb thumb drive;

e. One Kingston brand thumb drive metal finish;

f. One Kingston brand thumb drive with a Shawnee public schools label; and

g. One purple Lexar brand thumb drive 8 gb.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

Jurisdiction

7. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

8. The requested search is related to the following violations of federal law:

a. 18 U.S.C. §§ 1151, 1153, and 2241(c) (Aggravated Sexual Abuse of a Minor Under 12 Years of Age in Indian Country);
b. 18 U.S.C. §§ 1151, 1153, and 2244(a)(5) (Abusive Sexual Contact of a Minor Under 12 Years of Age in Indian Country);
c. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography)

9. Venue is proper because the property described in this affidavit is located within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

Definitions

10. The following definitions, inclusive of all definitions contained in 18 U.S.C. §§ 2246 and 2256, apply to this affidavit and the attachments incorporated herein:

a. The term "sexual act" means—

contact between the penis and the vulva or the penis and the anus, and for purposes of this subparagraph contact involving the penis occurs upon penetration, however slight;

contact between the mouth and the penis, the mouth and the vulva, or the mouth and the anus;

the penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person; or

the intentional touching, not through the clothing, of the genitalia of another person who has not attained the age of 16 years with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person;

b. The term "sexual contact" means the intentional touching, either directly or through the clothing, of the genitalia, anus, groin, breast, inner thigh, or buttocks of any person with an intent to abuse humiliate, harass, degrade, or arouse or gratify the sexual desire of any person;

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-

generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

d. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state;

e. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet;

f. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email

server, for as long a period of time as it takes to send or receive messages. One of the most commons methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;

g. A "hash value" or "hash ID" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;

h. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;

k. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; €(e) lascivious exhibition of the genitals or pubic area of any person; and

l. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Probable Cause

11. At all times relevant to this Affidavit, Harold James GRAHAM, DOB xx/xx/1963 ("GRAHAM"), was and is a member by blood of the Cherokee Nation of Oklahoma. GRAHAM lives on East Severn Street in Shawnee, Oklahoma, which is in Pottawatomie County and in the Western District of Oklahoma.

12. GRAHAM has two adult children: a daughter, B.S., and a son, A.G.

13. GRAHAM comes to visit and stay with B.S. and her family several times a year. B.S. has a four-year-old daughter, Minor Victim One (hereinafter MV 1).

14. B.S. and her family live on W. 126th Street South in Jenks, Oklahoma, located in the Northern District of Oklahoma and within the Muscogee (Creek) Nation Indian Reservation, which is Indian country as defined in 18 U.S.C. § 1151.

15. On July 29, 2022, B.S. contacted the Oklahoma Department of Human Services (OKDHS) about the sexual abuse of MV 1. B.S. learned of the abuse from MV 1's nanny. B.S. told OKDHS that the last time GRAHAM stayed at her house was from July 22 to July 28, 2022.

16. On August 9, 2022, Jenks Police Department (JPD) began an investigation based on reports from OKDHS. JPD interviewed MV 1's nanny, who recounted that MV 1 said she likes it when "Poppa Jamie" comes to visit because she likes "the cuddles" and when he "touches [her] peepee." "Poppa Jaime" is MV 1's nickname for GRAHAM.

17. MV 1's nanny explained what it looked like when GRAHAM touches MV 1's peepee. In response, MV 1 licked her fingers, rubbed them on top of her clothing over her genitals, and then licked her fingers again. MV 1 told her nanny that MV 1 "doesn't like it when it's hard, but [she] likes it when it's soft." The nanny believed MV 1 was referring to GRAHAM's penis. MV 1 told her nanny that GRAHAM touches MV 1 sometimes in the morning and sometimes in the afternoon. MV 1 denied that anyone else was around when GRAHAM touched her. On a later date, MV 1's nanny also told the JPD and the FBI that MV 1 showing the nanny

GRAHAM'S cell phone and noticed the screen saver was a picture of MV 1. The nanny recalled the incident because she thought the photo was very strange. The image depicted MV 1 laying on her stomach facing away from the camera with her buttocks as the focal point.

18. MV 1 was forensically interviewed on August 16, 2022. MV 1 did not disclose any information related to sexual abuse. Officers told B.S. to advise them if MV 1 made additional disclosures of sexual abuse in the future.

19. On November 14, 2022, MV 1 made another disclosure to her mother who reported it to JPD. B.S. told JPD that MV 1 stated she missed GRAHAM. MV 1 said she liked it when he licked his fingers and touched her peepee. A forensic interview was scheduled for later in the month.

20. On November 30, 2022, the JPD and the FBI attended MV 1's second forensic interview. MV 1 disclosed that GRAHAM would lick his fingers with his tongue then touch her peepee and her bum. MV 1 described that GRAHAM asked her in a quiet voice "is that good?" and "does that feel good?" MV 1 said, "it tickles, and feels funny and good." During the forensic interview, MV 1 was shown the illustration of a child's body and identified the peepee and bum as the vaginal and anal areas on the body. MV 1 identified the fingers as what GRAHAM would use to touch her.

21. On June 8, 2023, FBI interviewed B.S., who said GRAHAM was very affectionate and MV 1 would sit on his lap and cuddle with him on the couch when

he visited. B.S. stated that she was never abused by GRAHAM during her childhood.

22. B.S.'s recalled that her brother, A.G., told her that GRAHAM was investigated for sexually abusing another child in approximately June 2022. This investigation occurred in Shawnee, Oklahoma, and involved a child that GRAHAM babysat, four-year-old Minor Victim 2 (hereinafter MV 2). MV 2 is not related to GRAHAM. The report involved GRAHAM touching and attempting to touch four-year-old MV 2's private area on multiple occasions. The touches occurred when GRAHAM babysat MV 2 and her siblings. MV 2 told her guardian that GRAHAM would massage her back and tell her to undress. On August 30, 2022, MV 2 was forensically interviewed and disclosed that "Uncle James" kept touching her. MV 2 said it happened at his house. MV 2 expressed her discomfort with discussing Uncle James' touches throughout the interview and said that "Uncle James touches my bad part". MV 2 said Uncle James would have MV 2 sit on his lap and he would hug her tight and touch her bad part. MV 2 identified the "bad part" as her private area.

23. A.G. also told B.S. other facts about that investigation. A.G. said that GRAHAM gave A.G. a computer or pieces of a computer around the time of that investigation and that GRAHAM appeared nervous.

24. B.S. consented to a telephone conversation recording between her and GRAHAM. B.S. asked GRAHAM why MV 1 would say she was abused by him, specifically touching MV 1 on the genitals with his hand. GRAHAM replied he may have licked his fingers because he had food on his hand then cleaned MV 1 with a

wet wipe during a diaper change. B.S. told GRAHAM that MV 1 has not worn diapers in over a year, which GRAHAM acknowledged.

25. On June 8, 2023, B.S. told the FBI that she received a text message from GRAHAM that stated, "Hey thought about our conversation the other day, I did change the pull up one night and it may have been the night I had that snaggy nail. I asked you for the clippers in the morning."

26. On June 16, 2023, the FBI interviewed A.G. who stated he was never abused by GRAHAM. A.G. said he loaned GRAHAM a laptop in the past and would see if he could find it. A.G. believed his father gave him a desktop sometime in the past.

27. On June 28, 2023, A.G. provided the FBI with the Devices. Specifically, A.G. provided a black Dell Laptop computer that he loaned to GRAHAM for years.[1] A.G. signed a Consent to Search form for the laptop and said he wanted to help the investigation as much as he could. A.G. also turned over the six thumb drives described in Attachment A to the FBI. A.G. stated the thumb drives had been in the laptop bag when GRAHAM returned the laptop to A.G. and that the thumb drives had belonged to GRAHAM. A.G. stated he had previously told GRAHAM the thumb drives were in the bag, but GRAHAM told A.G. to keep the thumb drives with the bag and laptop.

28. A.G. said he looked through three of the six thumb drives out of curiosity. A.G. stated the purple thumb drive had multiple pornographic images saved on it.

[1] A.G. could not recall if this was the same computer GRAHAM gave to him in paragraph 19.

A.G. said he looked at some of the images. A.G. described the images he saw as a mix of adult pornographic images and what he described as "nudist colony" images that included images of naked children. He said he called them "nudist colony" pictures because one of the pictures had a sign that said, "Nudist Colony." A.G. said that the naked children looked young and undeveloped. A.G. said that in his opinion the images of the naked children were not sexually explicit; however, A.G. said he scrolled through only approximately 50 images before stopping because he felt uncomfortable viewing images of standard pornography mixed with images of naked children. A.G. said the other two of the three thumb drives he looked through had what appeared to be school and work items on them.

29. The Devices are currently in storage at the FBI Tulsa Resident Agency Property Room at 8023 East 63rd Place, Tulsa, Oklahoma. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

30. Based on my training and experience, it is reasonable to believe that GRAHAM has attempted to access, or successfully accessed, child sexual abuse material/child pornography. This belief is based on factors associated with this investigation. GRAHAM sexually abused two pre-pubescent children with whom he had only occasional access. Occasional access to children could increase the likelihood that GRAHAM would need to access child sexual abuse material/child pornography to further his sexual interest in children. A.G. also located nude

photographs of children, purportedly in a nudist colony. A.G. described that those photographs were interspersed with photographs of adult pornography. Although the pictures as described are not child sexual abuse material/child pornography, their proximity to what A.G. believed to be legal, adult sexually-stimulating material, suggests GRAHAM might have used those images in a sexual manner. Furthermore, A.G. is not a trained investigator or law enforcement officer and his description or belief that the images of the naked children on his father's device were not sexually explicit is not dispositive. That increases the likelihood that GRAHAM has accessed and possibly saved child sexual abuse material/child pornography on the laptop or flash drives.

Characteristics Common to Individuals Who Engage in the Sexual Exploitation of Children

31. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who sexually exploit children, either physically or through child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then

delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

f. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"[2] it;

[2] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United*

g. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user's identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may provide a window into the identities of individuals seeking to buy or sell child pornography online by tying the illicit transactions back to the user. Financial information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I know that individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers, cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

States v. Seiver, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

h. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, if Harold GRAHAM uses a portable device (such as a laptop computer) to access the internet and child pornography, and/or uses portable data storage devices (such as a laptop computer and flash drives) it is more likely than not that evidence of this access will be found on the Devices described in Attachment A.

Background on Child Pornography, Computers, the Internet, and Email

32. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, smartphones,[3] and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

[3] Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

b. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and laptop or tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, received, or accessed by anyone with access to a computer or smartphone;

c. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Photos may also be downloaded and stored on media storage devices like laptop computers and flash drives. Some media storage devices can easily be concealed and carried on an individual's person;

d. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

e. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and

f. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Technical Terms

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

34. Based on my training, experience, and research, I know that the Devices, specifically the Dell laptop computer, has capabilities that allow it to connect to and access the internet and other computers or wireless devices. I also know the Dell laptop computer can access, download, and upload content from the internet.

35. Based on my training, experience, and research, I know that the Devices, both the Dell laptop computer and the flash drives, can serve as digital storage devices that can store images, videos, and other electronic files.

36. In my training and experience, examining data stored on the Devices can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

Electronic Storage and Forensic Analysis

37. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

38. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

39. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as corroborative and/or direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who

used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

34. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution*. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is

reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

36. *Methods of examination*. In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Devices. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

37. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

38. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

Steve Colon
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to by phone on September 5, 2023.

SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

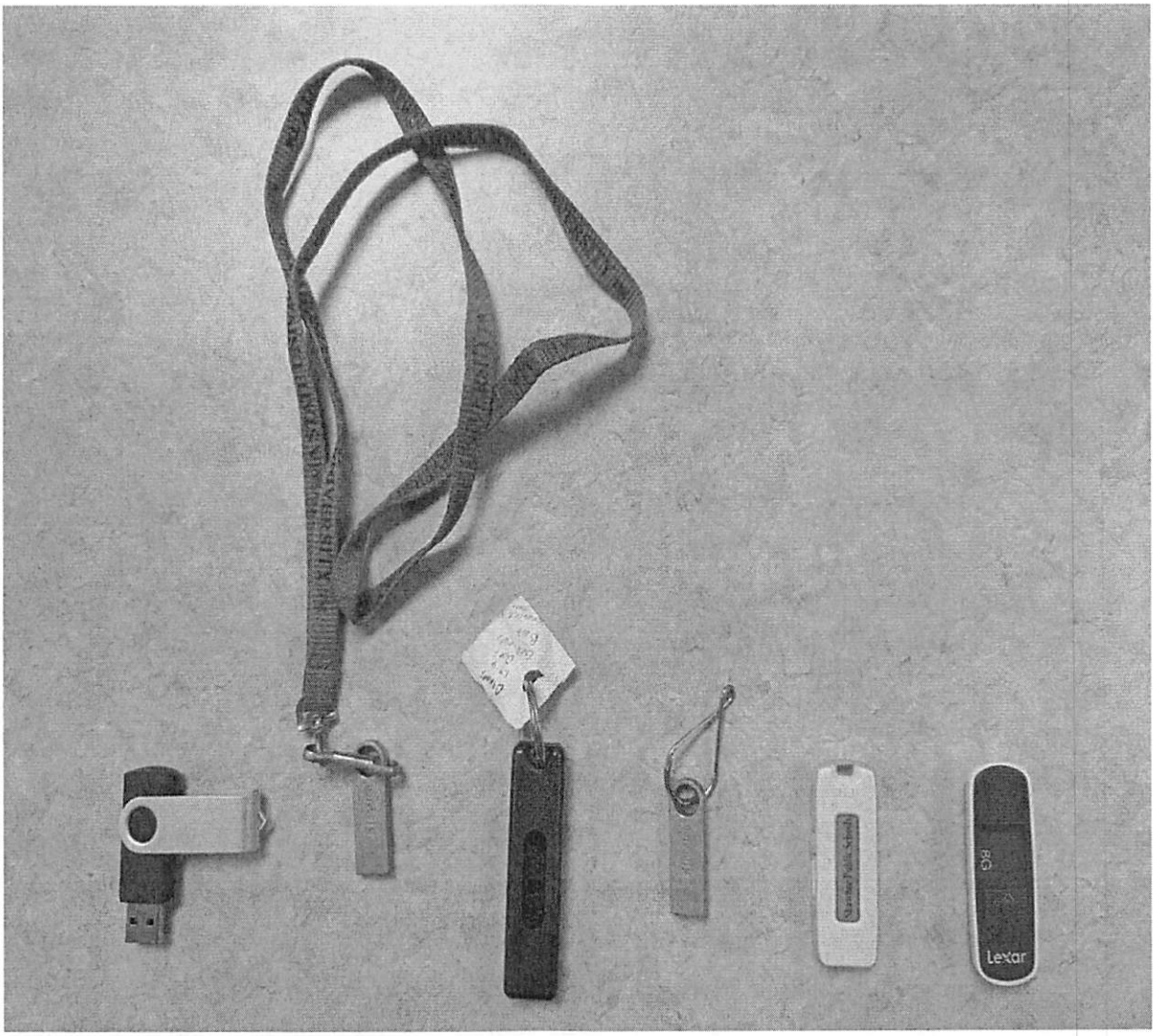
Property to be Searched

The property to be searched, hereinafter the "Devices" is listed below:

1. One black Dell laptop computer; product key tbfwd-w749m-qixvr-mwkew-cw6t3
2. One plain metal swivel thumb drive
3. One Kingston brand thumb drive with orange and black lanyard
4. One PNY brand black plastic optima pro 4gb thumb drive
5. One Kingston brand thumb drive metal finish
6. One Kingston brand thumb drive with a Shawnee public schools label
7. One purple Lexar brand thumb drive 8gb

The Devices are currently located at the FBI Tulsa RA Property Room, 8023 East 63rd Place, Tulsa, Oklahoma.

Images of Devices 2-7 are pictured below.



This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to the violations of Title 18, United States Code, Section § 2241(c) (Aggravated Sexual Abuse of a Minor Under 12 Years of Age in Indian Country), Title 18, United States Code, Section 2244(a)(5) (Abusive Sexual Contact of a Minor Under 12 Years of Age in Indian Country), and Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), including:

1. Records relating to the planning and execution of the criminal offense(s) above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
2. Application data relating to the criminal offense(s) above, which could include applications for capturing, viewing, or editing image, video, or audio files;
3. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
4. All records and information related to the geolocation of the Device(s);

5. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found;
6. Any and all electronic and/or digital records and/or documents of minor children, including MV 1 and MV 2, and nude minor children;
7. Any and all information, correspondence (including emails and text messages), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.